Published and Copyright (c) 1999 - 2014
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1651 12/19/14

~ Teens Fleeing Facebook ~ People Are Talking! ~ Hackers Have Serbia!
~ Weird Twist in Sony ~ Hackers Get into ICANN ~ Digital Privacy?
~ Miyamoto on "Amiibo"! ~ E.T. to Smithsonian! ~ HTTP Pages Insecure?

~ A Duck Hunt Christmas! ~ Router Vulnerability! ~ Windows 10 Leaked!

-* Net Neutrality Regs Essential *-
-* FBI Blames North Korea for Sony Hack *-
-* Congress Passes Four Cybersecurity Bills! *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""""

The world is abuzz over the news that North Korea is allegedly responsible for hacking Sony recently. And, the hackers have further caused "damage" with threats should Sony release their pending movie. "The Interview."

While I understand Sony's hesitance to release the movie as scheduled, I have some doubts that the move is totally the correct one. While it's true that the hackers have the potential to create a lot more problems, should we be intimidated to the point and position Sony finds itself? This could be considered a form of terrorism, I guess. And what has the world said to terrorism? I guess we'll see where this prediament takes Sony, and the world.

The holiday season is in full swing. Happy Hanukkah to everyone who celebrates. And, X-mas is next week, so I wish to convey holiday greetings in that regard, as well.

Until next time...

=~=~=~=

->In This Week's Gaming Section - Miyamoto on 'Amiibo,' 'Zelda' and 'Mario' Movie!
""""""""""""""""""""""""""""""" Unearthed E.T. Atari Cartridge Phones Home to Smithsonian!
Nintendo Is Rereleasing Duck Hunt on Christmas Day!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""

Miyamoto on ’Amiibo,’ ’Zelda’ and ’Mario’ Movie

Shigeru Miyamoto seems giddy and with good reason.

The veteran Nintendo designer behind such landmark video-game franchises as "Mario Bros." and "Donkey Kong" is happy that after three years of sluggish sales for Nintendo’s touchscreen-centric Wii U console, the Kyoto, Japan-based gaming giant is bouncing back, just like the famous springy plumber dreamed up 33 years ago by Miyamoto.

With the recent popularity of "Super Smash Bros." and "Mario Kart 8," as well as the successful launch of the "amiibo" interactive toy figure line, Miyamoto has a few reasons to smile.

Over a cup of coffee, Miyamoto as translated by Nintendo product marketing director Bill Trinen discussed the possibilities for "amiibo," the latest installment of "The Legend of Zelda" and the future of the "Mario" franchise.

AP: It sounds like "amiibo" has been a success since it launched with "Smash Bros." You’ve announced that "amiibo" will be compatible with upcoming games like "Mario Party 10" and "Yoshi’s Woolly World," but how else do you see the figures being utilized in the future?

Miyamoto: We’ll continue to make future games that will have functionality with the "amiibo" characters as an additional present for people who bought them. Beyond that, we’re looking at how we can use the "amiibo" functionality in the future, including cards and whatnot.

AP: If you discontinue certain "amiibo" figures, will you continue to include them digitally in future games?

Miyamoto: We’re not making promises for certain figures, but the way "amiibo" is designed is that certain games can have "amiibo" specifically for that game. Other games can take advantage of past "amiibo" that developers want to make their game compatible with. In the future, we have the option, if certain "amiibo" figures are no longer available in stores, to release an "amiibo" in card form with the same functionality.

AP: You recently previewed gameplay footage from next year’s "Zelda" installment. What’s your strategy for "Zelda" on the Wii U?

Miyamoto: One of the main things we wanted to do was go back to the open-world concept of the original "Zelda" games and design with that in mind. That’s really the direction the team is going in. This time, we’ve brought back Link’s horse, Epona, and his bow and arrow, but what we’ve decided is really fun is being able to freely walk around in this world and choose what you want to do and how you want to explore. I can’t talk much about it, but one of the things we’re working on right now is that, as you play, the world will change and be affected by what you choose to do.

AP: You’re personally working on a new "Star Fox" game now. It feels like a long time since we’ve seen Fox piloting his Arwing. What’s he up to now?

Miyamoto: I like to create gameplay mechanics more than I do stories. The

story might not be too different from past "Star Fox" games, but the gameplay mechanics are going to feel very different because of the two-screen system of the Wii U with the GamePad and TV screen. It'll make for a very fun and unique way to play.

AP: There was correspondence that came out of the Sony leak that mentioned "Spider-Man" producer Avi Arad was working on a "Mario Bros." animated film. Is that true? If so, what would your role be in the film, and what do you envision a modern "Mario" film would look?

Miyamoto: I heard something about that this morning. What's interesting is that over the past 20 years, people come to us on a fairly regular basis about creating "Mario" movies. There are times that those ideas end right when they bring them to us, and other times we'll listen to presentations. It's not very unusual, and it's something we've been doing for a very long time. I don't particularly have a vision that the next iteration of "Mario" is going to be in film.

AP: Mario has been busy on the Wii U with "Super Mario 3D World" last year and now "Mario Kart 8." Is he taking the next year off? What can we expect from that franchise in the future?

Miyamoto: Since we first created Mario, people have compared him to Mickey Mouse. I've always said Mickey Mouse evolved with each evolution in animation. You saw Mickey Mouse each step of the way. From early on, I wanted Mario to be that character in the digital world, so that with each digital evolution, he was there to usher in the next era. I think that maybe when we release the next hardware system, you can look forward to seeing Mario take on a new role or in a new game.

AP: I know you're working on "Star Fox," but beyond that, will you continue to design games for the Wii U, or are you already thinking about new hardware?

Miyamoto: We're focused on providing a robust line-up of Wii U software for next year. It seems like we've managed to do that this year and people are very happy with what we've done on Wii U. For the time being, our focus is on the Wii U hardware, but Nintendo as a whole has groups working on ideas for new hardware systems. While we're busy working on software for the Wii U, we have production lines that are working on ideas for what the next system might be.

Nintendo Is Rereleasing Duck Hunt on Christmas Day

There are few better ways to spend the holidays than shooting birds so it s only natural that Nintendo is bringing its classic Duck Hunt to the Wii U on Dec. 25. The game will be available through the Virtual Console service starting on Christmas Day, and you ll be able to use a Wii remote in place of the iconic orange-and-gray NES Zapper light gun that worked with the original. It should make a great complement to new Wii U releases like Super Smash Bros. and Captain Toad: Treasure Tracker.

No word on the price, though NES games typically sell for $4.99 through the Virtual Console, which is a small price to pay for reliving a classic just remember that this is a straight port of the original, so you still can t shoot the dog.

=~=~=~=

->A-ONE Gaming Online - Online Users Growl & Purr!
"""""""""""""""""""""

Unearthed E.T. Atari Cartridge Phones Home to Smithsonian

One man’s trash is another museum’s treasure. The Smithsonian has snagged a copy of the E.T. the Extra Terrestrial Atari 2600 video game, one of many that were unearthed in a New Mexico landfill earlier this year.

The game is set for display in The National Museum of American History in Washington, D.C.

As part of a documentary, the (now-defunct) Microsoft Xbox Entertainment Studios chased rumors that Atari dumped 14 truckloads of unsold cartridges and other equipment in a New Mexico landfill in 1983.

"Thinking that it would be forever buried in the desert if it was there, I put it [the E.T. game] down on my list to collect," Smithsonian technician Drew Robarge wrote in a blog post.

He contacted Microsoft’s crew and requested a copy of the legendarily awful game for the museum, "but I knew that my chances of getting one were slim to none," he said.

But the studio’s and Robarge’s efforts paid off in April, when an organized dig found a number of Atari titles, including copies of E.T., which had dismal sales in 1982 and reportedly contributed to the demise of the Atari 2600 console.

"The Smithsonian is no hall of fame it’s our job to share the complicated technological, cultural, and social history of any innovation, including video games," Robarge said.

Which is why curators are excited to add to their collection the E.T. Atari title, which the museum specialist said "personifies the video game crash that took place from 1982 to 1985."

The Smithsonian isn’t the only one looking to collect a piece of gaming history: In early November, the Tularosa Basin Historical Society of Alamogordo launched eBay auctions for about 100 unearthed titles, including E.T. Buyers will receive the game as portrayed in the photos which, in almost every case, is more than gently used. Each title also comes with a narrative with photos of the 1983 burial and the 2014 excavation, "proving the legend true."

Starting prices range from $35 to $75, and each game includes a certificate of authenticity. Almost two months later, the E.T. title remains the most popular, with bids reaching $200 to $400.

"The [E.T. Atari 2600] cartridge is one of the defining artifacts of the crash and of the era," Robarge wrote in the blog. "In addition to the

crash, the cartridge can tell many stories: the ongoing challenge of making a good film to a video game adaptation, the decline of Atari, the end of an era for video game manufacturing, and the video game cartridge life cycle."

It also provides closure, he said, regarding the burial's urban legend, the golden years of Atari, and the American-dominated era of game consoles.

"All of these possible interpretations make for a rich and complicated object," Robarge said. "As they say, one man's trash is another man's treasure."

If you can't make it to D.C. to check out the famed cartridge in person, Xbox Live members can learn more about the burial and excavation in the Atari: Game Over documentary, available to view on Xbox consoles and online.

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Sony Pictures Hack Takes Yet Another Weird Twist

The Sony Pictures Entertainment hack has taken yet another weird twist with hackers apparently offering to withhold data stolen from the company s employees.

On Sunday the group claiming responsibility for the crippling Nov. 24 hack offered not to release some email correspondence from Sony Pictures' employees. The group urged employees to contact them if they don t want their correspondence released.

There was no way to determine how many, if any employees, had supplied their details.

The post, which claimed to be from the shadowy Guardians of Peace, or GOP, group, appeared on file sharing sites Pastebin and Friendpaste, according to the website Recode.

Message to SPE Staffers, it read. We have a plan to release emails and privacy of the Sony Pictures employees. If you don t want your privacy to be released, tell us your name and business title to take off your data.

Sunday s message also contained links to several file sharing sites for obtaining the group s latest leaks. Clearly keen to maintain the pressure on Sony, the group vowed to release larger quantities of data, which it described as a Christmas gift, reiterating a similar GOP message posted on Saturday.

Experts have noted the resolve of the attack s perpetrators, who seem

intent on prolonging Sony s pain.

Whoever it is, they must feel like they are immune to retaliation, Jim Lewis, director and senior fellow at the Center for Strategic and International Studies, told FoxNews.com, in an email. They are also really motivated to keep it up this long most of these incidents are more like smash-and-grab.

Sunday s post is the latest in a flurry of cyber assaults aimed at Sony Pictures, which have included leaks of confidential data and unreleased movies, as well as threats against Sony employees. The producers of James Bond films have also acknowledged that an early version of the screenplay for the new movie "Spectre" was among the material stolen in the massive Sony Pictures cyberattack.

Sony is receiving repeated body blows from the breach, which is perhaps indicative of the intention to damage the reputation of the company, wrote Chris Boyd, malware intelligence analyst at Malwarebytes Labs, in an email to FoxNews.com. Typically a big company breach is all about stealthy data theft and low profile operations, however in this case the motivation appears focused on creating crippling headlines - it could almost be the beginning of a Bond film itself.

The finger of suspicion has already been pointed at North Korea over the hack, although Sony Pictures recently denied a report that it was poised to blame Pyongyang for the attack. The studio s forthcoming film The Interview, starring Seth Rogen and James Franco as journalists enlisted to assassinate dictator Kim Jong-un, has outraged North Korea.

There has also been plenty of speculation that the cyberattack was an inside job.

With the shockwaves from the hack still reverberating, Sony Pictures has reportedly demanded that at least three media outlets stop reporting stories based on documents obtained by hackers.

The Center for Strategic and International Studies Lewis told FoxNews.com that the attack has also shone a spotlight on hackers use of file sharing sites such as Pastebin.

While Saturday and Sunday s GOP posts have been removed from Pastebin, a GOP message titled Gift of Sony for the 8th day: GOP at Christmas (2), which apparently corresponds to Sunday’s Pastebin message, is still available on Friendpaste.

A spokesman for Pastebin told FoxNews.com that it received two requests about the posts related to the Digital Millennium Copyright Act (DCMA). "We always comply with such request when the items in question contain sensitive data," he added, in an email to FoxNews.com.

Friendpaste was unavailable for comment.

FBI Blames North Korea for Sony Hack

The US Federal Bureau of Investigation says North Korea was behind a cyber-attack on Sony Pictures over a film about its leader Kim Jong-un.

The agency said analysis of malware showed links to North Korea.

Sony withdrew the film The Interview following threats from hackers, who had earlier also released sensitive information stored on Sony computers.

CNN quoted the hackers as welcoming the withdrawal and warning Sony not to release the film in any form.

The emailed message was received by Sony's top executives on Thursday night and was obtained by CNN.

US President Barack Obama is scheduled to address reporters on Friday afternoon, where he is expected to face questions on the matter.

Sony's decision has outraged many artists. Actor George Clooney told the trade website Deadline on Thursday that the film should be released online.

Earlier the White House labelled the Sony breach a serious national security matter.

On Thursday, White House spokesman Josh Earnest told reporters US officials had held daily discussions about the Sony cyber-attack and were considering an "appropriate response".

Sony cancelled the holiday release of the comedy film after national theatre chains refused to show it.

The movie features James Franco and Seth Rogen as two journalists who are granted an audience with North Korean leader Kim Jong-un.

The CIA then enlists the pair to assassinate him. The film was due to have been released over Christmas.

Hackers had earlier issued a warning referring to the 11 September 2001 terror attacks, saying "the world will be full of fear" if the film was screened.

The film's cancelled release drew criticism in Hollywood, with some calling it an attack on the freedom of expression.

Actor George Clooney told the trade website Deadline on Thursday the film should be released online, saying Hollywood shouldn't be threatened by North Korea.

In November, a cyber-attack crippled computers at Sony and led to upcoming films and workers' personal data being leaked online.

The hackers also released salary details and social security numbers for thousands of Sony employees - including celebrities.

North Korea earlier this month denied involvement in the hack - but praised the attack itself as a "righteous deed".

An article on North Korea's state-run KCNA news agency, quoting the country's top military body, said suggestions that Pyongyang was behind the attack were "wild rumour".

However, it warned the US that "there are a great number of supporters and sympathisers" of North Korea "all over the world" who may have

carried out the attack.

In the article, Sony Pictures was accused of "abetting a terrorist act" and "hurting the dignity of the supreme leadership" of North Korea by producing the movie.

FBI Update on Sony Investigation

Today, the FBI would like to provide an update on the status of our investigation into the cyber attack targeting Sony Pictures Entertainment (SPE). In late November, SPE confirmed that it was the victim of a cyber attack that destroyed systems and stole large quantities of personal and commercial data. A group calling itself the Guardians of Peace claimed responsibility for the attack and subsequently issued threats against SPE, its employees, and theaters that distribute its movies.

The FBI has determined that the intrusion into SPE s network consisted of the deployment of destructive malware and the theft of proprietary information as well as employees personally identifiable information and confidential communications. The attacks also rendered thousands of SPE s computers inoperable, forced SPE to take its entire computer network offline, and significantly disrupted the company s business operations.

After discovering the intrusion into its network, SPE requested the FBI s assistance. Since then, the FBI has been working closely with the company throughout the investigation. Sony has been a great partner in the investigation, and continues to work closely with the FBI. Sony reported this incident within hours, which is what the FBI hopes all companies will do when facing a cyber attack. Sony s quick reporting facilitated the investigators ability to do their jobs, and ultimately to identify the source of these attacks.

As a result of our investigation, and in close collaboration with other U.S. government departments and agencies, the FBI now has enough information to conclude that the North Korean government is responsible for these actions. While the need to protect sensitive sources and methods precludes us from sharing all of this information, our conclusion is based, in part, on the following:

Technical analysis of the data deletion malware used in this attack revealed links to other malware that the FBI knows North Korean actors previously developed. For example, there were similarities in specific lines of code, encryption algorithms, data deletion methods, and compromised networks.

The FBI also observed significant overlap between the infrastructure used in this attack and other malicious cyber activity the U.S. government has previously linked directly to North Korea. For example, the FBI discovered that several Internet protocol (IP) addresses associated with known North Korean infrastructure communicated with IP addresses that were hardcoded into the data deletion malware used in this attack.

Separately, the tools used in the SPE attack have similarities to a cyber attack in March of last year against South Korean banks and media outlets, which was carried out by North Korea.

We are deeply concerned about the destructive nature of this attack on a

private sector entity and the ordinary citizens who worked there. Further, North Korea s attack on SPE reaffirms that cyber threats pose one of the gravest national security dangers to the United States. Though the FBI has seen a wide variety and increasing number of cyber intrusions, the destructive nature of this attack, coupled with its coercive nature, sets it apart. North Korea s actions were intended to inflict significant harm on a U.S. business and suppress the right of American citizens to express themselves. Such acts of intimidation fall outside the bounds of acceptable state behavior. The FBI takes seriously any attempt whether through cyber-enabled means, threats of violence, or otherwise to undermine the economic and social prosperity of our citizens.

The FBI stands ready to assist any U.S. company that is the victim of a destructive cyber attack or breach of confidential business information. Further, the FBI will continue to work closely with multiple departments and agencies as well as with domestic, foreign, and private sector partners who have played a critical role in our ability to trace this and other cyber threats to their source. Working together, the FBI will identify, pursue, and impose costs and consequences on individuals, groups, or nation states who use cyber means to threaten the United States or U.S. interests.

Hackers Trick Way into ICANN Computers

The private agency that acts as a gatekeeper for the Internet said that hackers tricked their way into its computers.

A "spearfishing" attack aimed at US-based nonprofit Internet Corporation for Assigned Names and Numbers (ICANN) hooked staff members with emails crafted to appear as though they were sent from peers using "icann.org" addresses, according to a blog post.

"The attack resulted in the compromise of the email credentials of several ICANN staff members," ICANN said.

It appeared that the attack commenced in November. Typically, spearfishing attacks dupe people into clicking on links to what appeared to be legitimate email log-in pages but aren’t or open attached files booby-trapped with viruses.

The ruse won hackers ICANN email user names and passwords, giving the intruders control of accounts and keys to reaching deeper, according to the blog post.

User names and passwords were used this month to access a Centralized Zone Data System, where hackers could get hold of files about generic top-level domains as well as names, addresses, passwords and other valuable information about users, according to ICANN.

Hackers were also said to have used compromised passwords to get into an ICANN wiki page; its blog, and a Whois index of registered owners of web addresses.

The blog and Whois did not appear to have been tampered with, according to ICANN, which provided no insight into who was behind the attack.

ICANN believed that security enhancements made earlier this year limited how deep hackers could dive into its computers. More defense measures have been instituted since the hack, according to ICANN.

The organization’s chief security officer is Jeff Moss, who founded the notorious annual Def Con gathering of hackers in Las Vegas and has the hacker name Dark Tangent.

ICANN, which is in charge of assigning Internet domain names, is expected to break free of US oversight late next year.

Washington said in March it might not renew its contract with the Los Angeles-based agency, provided a new oversight system is in place that ensures the Internet addressing structure is reliable.

The agency plans to submit a proposal on oversight to the US Department of Commerce next year.

Serbia Hackers Claimed To Have Stolen The Entire National Database

A group of hackers claims to have compromised the national database system stolen all information related to citizens resident in Serbia.

Hackers claim to have data about all citizens in Serbia, if the news is confirmed this is another clamorous data breach that could have serious repercussion on the Government.

It seems that cyber criminals hacked the Serbian State s network, accessed to the identities of almost all Serbians, which are now exposed to risks of frauds and identity theft. Five hackers have claimed they hacked the internet backbone of the Serbian Identity system and stolen ID numbers of almost all citizens of Serbia. Though the has not been confirmed by the Serbian authorities, the hackers have leaked a screenshot of what seems to be details of Serbian citizens.

The crew of cybercriminals that claim for the attack on the State s network of Serbia is composed of five hackers that claimed that they violated the internet backbone of the Serbian Identity system and stolen ID numbers of almost all citizens of the country. An the time I m writing, the Government of Serbia hasn t confirmed the data breach, meanwhile the hackers have leaked online a screenshot of the alleged list displaying data of Serbian citizens.

The hackers have announced the data breach via email to the Serbian daily Blic, as reported also by the news portal InSerbia.

We have whole Serbia in our hand. We have almost all information about the Serbian citizens starting from ID numbers to what they do, where they work, live, their phone numbers . is reported in the email.

The image reporting a table of the Serbian national archive was attached to the email, it contains data of Serbian citizens living in different cities of the country.

The hackers seem to be Serbians that protest against national cyber police because it is more interested in the persecution of national hackers instead Albanian cyber criminal crews.

We show this information in public for many reasons. The first and main reason is that our cyber police chases exclusively Serbian hackers while it ignores Albanian hackers. Now they will have more than specific reason to look for us, but they will waste their time, states the email.

The hackers have alleged also other motivations to the patriotic attack, they declared to have hit the national database also to demonstrate that the Serbian cyber system is vulnerable.

The third reason is that the state sees, and after multiple warnings realizes, that the security of the system is weak and that they should take more care about it, the e-mail reads.

If the data breach is confirmed, the possible consequences for the population are dramatic. Unaware people could be targeted by cyber criminals that could be used the stolen data for illegal activities. The economic impact is severe, something similar happened to South Korea, where national ID system was compromised, causing the exposure of as much as 80 per cent of the population.

Modernizing the whole nation system will have a great economic impact, it would cost to the South Korea about $650 million.

Router Vulnerability Puts 12 Million Home and Business Routers at Risk

More than 12 million routers in homes and businesses around the world are vulnerable to a critical software bug that can be exploited by hackers to remotely monitor users traffic and take administrative control over the devices, from a variety of different manufacturers.

The critical vulnerability actually resides in web server "RomPager" made by a company known as AllegroSoft, which is typically embedded into the firmware of router , modems and other "gateway devices" from about every leading manufacturer. The HTTP server provides the web-based user-friendly interface for configuring the products.

Researchers at the security software company Check Point have discovered that the RomPager versions prior to 4.34   software more than 10 years old   are vulnerable to a critical bug, dubbed as Misfortune Cookie. The flaw named as Misfortune Cookie because it allows attackers to control the "fortune" of an HTTP request by manipulating cookies.

The vulnerability, tracked as CVE-2014-9222 in the Common Vulnerabilities and Exposures database, can be exploited by sending a single specifically crafted request to the affected RomPager server that would corrupt the gateway device’s memory, giving the hacker administrative control over it. Using which, the attacker can target any other device on that network.

"Attackers can send specially crafted HTTP cookies [to the gateway] that exploit the vulnerability to corrupt memory and alter the application and system state," said Shahar Tal, malware and vulnerability research manager with Check Point. "This, in effect, can trick the attacked device to treat the current session with administrative privileges - to the misfortune of the device owner.

Once attackers gain the control of the device, they could monitor victims' web browsing, read plaintext traffic traveling over the device, change sensitive DNS settings, steal account passwords and sensitive data, and monitor or control Webcams, computers, or other network connected devices.

At least 200 different models of gateway devices, or small office/home office (SOHO) routers from various manufacturers and brands are vulnerable to Misfortune Cookie, including kit from D-Link, Edimax, Huawei, TP-Link, ZTE, and ZyXEL.

The bug not only affects routers, modems and other gateway devices, but anything connected to them from PCs, smartphones, tablets and printers to "smart home" devices such as toasters, refrigerators, security cameras and more. This simply means if a vulnerable router is compromised, all the networked device within that LAN is at risk.

Misfortune Cookie flaw can be exploited by any attacker sitting anywhere in the world even if the gateway devices are not configured to expose its built-in Web-based administration interface to the wider Internet, making the vulnerability more dangerous.

Because many routers and gateway devices are configured to listen for connection requests publicly on port 7547 as part of a remote management protocol called TR-069 or CWMP (Customer Premises Equipment WAN Management Protocol), allowing attackers to send a malicious cookie from far away to that port and hit the vulnerable server software.

The critical vulnerability was introduced in 2002, and AllegroSoft apparently fixed the bug in its RomPager software back in 2005, but hardware from major companies such as Huawei, D-Link, ZTE and others currently sell products contains the vulnerable versions of RomPager. As demonstrated by Check Point's finding that 12 million vulnerable gateway devices in homes, offices and other locations still exist.

"We believe that devices exposing RomPager services with versions before 4.34 (and specifically 4.07) are vulnerable. Note that some vendor firmware updates may patch RomPager to fix Misfortune Cookie without changing the displayed version number, invalidating this as an indicator of vulnerability."

"Misfortune Cookie is a serious vulnerability present in millions of homes and small businesses around the world, and if left undetected and unguarded, could allow hackers to not only steal personal data, but control peoples homes," Tal said.

So far, Check Point has not observed an attack involving Misfortune Cookie in the wild, but the company is having a close look on the older unresolved issues in which routers and gateway devices were compromised in different and unknown ways.

New Research Reveals More than Three Quarters of Organizations Have Suffered a DNS Attack

Seventy-six percent of organizations in the U.S. and U.K. have suffered a Domain Name System (DNS) attack, with 49 percent experiencing one in the past 12 months. The most common DNS threats reported were DDoS

(74 percent), DNS exfiltration (46 percent), DNS tunneling (45 percent) and DNS hijacking (33 percent) by those who had suffered an attack. That’s according to an independent research study undertaken by Vanson Bourne and commissioned by Cloudmark, Inc.

Three hundred IT decision makers were polled across the U.S. and U.K. and, of those who reported suffering a DNS attack, more than half admitted to losing business critical data or revenue. An astounding third of respondents also confirmed they had lost confidential customer information. Despite these serious business implications, 44 percent of those who found it difficult to justify DNS security investment to their company felt it was because their senior management do not see DNS security as an issue and are, in fact, considered barriers to investment. This is in spite of more than half of the IT decision makers polled (55 percent) citing the theft of private or confidential data as a major concern to their organization.

"The survey findings suggest that large organizations are not only inadequately protecting company intellectual property against DNS attacks but more needs to be done to help educate businesses on the methods used by DNS attackers," said Neil Cook, chief technology officer at Cloudmark.

"While DDoS threats continue to be a common method of attack to siphon off valuable resources, organizations need to review their security solutions to ensure they can protect against a multitude of other attacks including DNS exfiltration and DNS tunneling, particularly in industries where high-value data is held, such as retail and financial industries. Once an organization’s data is in the hands of cyber-criminals, the brand reputation, customers and ultimately revenue of that organization can be severely affected."

Additional findings from the research include:

Shockingly, in the U.S., 66 percent of respondents have experienced a DNS attack in the past 12 months.

Of more concern, 23 percent of U.K. respondents admitted they did not know if their organization had ever suffered a DNS attack.

Retail, distribution and transport firms reported the highest instance of DNS attacks of all vertical industries polled, with 74 percent suffering from an attack in the past 12 months. The industry also revealed itself as the biggest victim of DNS exfiltration attacks (56 percent), with financial services organizations a close second (51 percent) of those who had been victim to an attack.

Customer retention and brand reputation were the top concerns reported following a DNS attack.

For more information about the impact of DNS threats, please visit: https://www.cloudmark.com/en/register/whitepapers/infonetics-protecting-dns-infrastructure/direct/pdf.

Congress Passes Four Cybersecurity Bills

Congress approved a package of four cybersecurity bills after a series of votes in the House and Senate this week, increasing the likelihood that

some cybersecurity-related legislation will be enacted by the end of the year. None of the bills address some of the larger, more contentious cybersecurity issues, such as immunity for private companies that share cybersecurity threat information with the federal government. Instead, the bills focus on narrower cybersecurity issues and the structures and procedures of the federal agencies that oversee cybersecurity. Two of the measures, S. 2519 and S. 2521, are primarily focused on centralizing the federal government s cybersecurity efforts and enhancing information sharing with the private sector, while the remaining bills, S. 1691 and H.R. 2592, are focused on strengthening the Department of Homeland Security s cybersecurity workforce and recruitment efforts.

For the private sector, the most significant of the four bills is the National Cybersecurity Protection Act of 2014, S. 2519, which would codify the Department of Homeland Security s existing National Cybersecurity and Communications Integration Center (NCCIC). The NCCIC would provide a platform for the government and private sector to share information about cybersecurity threats, incident response, and technical assistance. The bill requires the Center to include representatives of federal agencies, state and local governments, and private sector owners and operators of critical information systems. However, the bill gives the Undersecretary of Homeland Security discretion about including governmental or private entities in the center s operations.

The House also passed the Federal Information Security Modernization Act of 2014, S. 2521, which amends the 2002 Federal Information Security Management Act to centralize federal government cybersecurity management within the Department of Homeland Security. The bill maintains the Director of the Office of Management and Budget s existing authority over federal civilian agency information security policies while delegating authority to the Homeland Security Secretary to implement these policies. The bill also delegates implementation authority for defense-related and intelligence-related information security to the Secretary of Defense and the Director of National Intelligence, respectively. The bill also codifies the OMB s directive, issued this past October, that gives DHS authority to scan the networks of other federal civilian government agencies. Both S. 2521 and S. 2519 passed the Senate earlier in the week and now await the President s signature.

In addition, the House passed two bills that focus on strengthening the federal government s cybersecurity workforce. S. 1691, which includes provisions from the DHS Cybersecurity Workforce Recruitment and Retention Act, would improve hiring procedures and compensation ranges for cybersecurity positions at the Department of Homeland Security. Under the provisions of the bill, the Department of Homeland Security is required to pay cybersecurity workers similar to the salary that cybersecurity positions receive in the Defense Department.

The bill also requires DHS to file annual reports on its recruitment and retention of cybersecurity workers. The House also passed H.R. 2952, the Cybersecurity Workforce Assessment Act, as amended by the Senate. The bill would require the Department of Homeland Security to conduct an assessment of its cybersecurity workforce every three years, in addition to developing a strategy for enhancing the recruitment and training of cybersecurity employees. Both bills previously passed the Senate and now await the President s signature.

FCC Chair Tells Congress Net Neutrality Regs 'Essential'

New Net neutrality rules are essential to protect openness on the Web, Federal Communications Commission Chairman Tom Wheeler said in a new letter to Congress.

I believe that the Internet must remain an open platform for free expression, innovation, and economic growth, Wheeler wrote to Rep. Bob Goodlatte (R-Va.) in a letter dated Dec. 9 and made public this week. We cannot allow broadband networks to cut special deals to prioritize Internet traffic and harm consumers, competition, and innovation.

Wheeler's statement comes in response to a letter from Goodlatte expressing support for the idea that existing antitrust laws can achieve the same goals as new Net neutrality rules.

Strong enforcement of the antitrust laws can prevent dominant Internet service providers from discriminating against competitors' content or engaging in anticompetitive pricing practices, Goodlatte, chairman of the House Judiciary Committee, wrote to the FCC last month.

Antitrust law prosecutes conduct once it occurs, by determining on a case-by-case basis whether parties actually engaged in improper conduct, the lawmaker added. Regulation, by contrast, is a blunt, 'one size fits all' approach that creates a burden on all regulated parties.

Goodlatte has expressed similar views in the past, including at a Congressional hearing this summer.

Wheeler responded last week that Net neutrality rules can work in tandem with antitrust law to promote open Internet principles.

There has been a decade of consistent action by the Commission to protect and promote the Internet as an open platform for innovation, competition, economic growth, and free expression, Wheeler wrote. At the core of all of these Commission efforts has been a view endorsed by four Chairmen and a majority of the Commission's members in office during that time: that FCC oversight is essential to protect the openness that is critical to the Internet's success.

The FCC pass Net neutrality rules in 2010, but those regulations were struck down in January by the D.C. Circuit Court of Appeals. Since then, the agency has been trying to craft new broadband regulations that will hold up in court.

Earlier this year, Wheeler proposed a set of controversial rules that would prohibit broadband providers from blocking or degrading material, but would allow them to charge companies extra fees for faster delivery.

That proposal drew criticism from many net neutrality proponents, who say that the FCC should also ban paid fast lanes. Last month, President Barack Obama publicly urged the FCC to ban paid prioritization deals.

The FCC is expected to vote on the issue early next year.

Can Digital Privacy Exist When Life Online Is Public by Nature?

Is privacy possible in an increasingly interconnected world? Experts aren t particularly optimistic in a new poll conducted by the Pew Research Internet Project, 55 percent of Internet and security experts predicted that policymakers and technologists would not be able to create a basic, unified privacy-rights infrastructure by 2025.

The poll encompasses 2,511 responses from experts on security, privacy, and freedom in the online world, many of whom said that online life is public by nature, and that upcoming generations will not value privacy the same way current generations do.

In order to exist online, you have to publish things to be shared, and that has to be done in open, public spaces, writes GigaOm lead researcher Stowe Boyd as part of the poll results, adding that people give up a certain amount of privacy in order to find friends and conduct business online.

The poll s respondents also noted that many popular businesses and services rely on the capture of personal information as part of their business model. Tech companies such as Google and Facebook aggregate user information to sell to advertisers, who then create targeted ads based on demographic information and browsing habits. Traditional retail, entertainment, and insurance companies are also relying more and more on the capture of user information as part of their business models.

Most respondents also agreed that people are generally willing to give up personal information simply for the sake of convenience.

[M]ost people s life experiences teach them that revealing their private information allows commercial (and public) organisations to make their lives easier (by targeting their needs), whereas the detrimental cases tend to be very serious but relatively rare, writes Bob Briscoe, a chief researcher for British Telecom, in the survey.

It s worth pointing out that the survey was not necessarily a representative sample of expert views: Pew refers to their method as a canvassing, since the organization invited experts to weigh in on the question rather than conducting a randomized, controlled survey. Nevertheless, most respondents agreed that while online life is public by nature, an international privacy framework is needed to ensure security and continued innovation.

Last month the United Nations approved a resolution that would call on member states to protect citizens right to online privacy. Sponsored by Germany and Brazil, the Right to privacy in the digital age resolution follows on a similar measure calling on states to respect human rights online. The latter resolution passed after former National Security Agency contractor Edward Snowden leaked information about surveillance practices in the United States and elsewhere.

Chrome Plans To Mark All ’HTTP’ Traffic as Insecure from 2015

Google is ready to give New Year gift to the Internet users, who are concerned about their privacy and security. The Chromium Project’s security team has marked all HTTP web pages as insecure and is planning to explicitly and actively inform users that HTTP connections provide no

data security protections.

There are also projects like Let’s Encrypt, launched by the non-profit foundation EFF (Electronic Frontier Foundation) in collaboration with big and reputed companies including Mozilla, Cisco, and Akamai to offer free HTTPS/SSL certificates for those running servers on the Internet at the beginning of 2015.

This is not the first time when Google is taking initiative to encourage website owners to switch to HTTPS by default. Few months ago, the web Internet giant also made changes in its search engine algorithm in an effort to give a slight ranking boost to the websites that use encrypted HTTPS connections.

"We, the Chrome Security Team, propose that user agents (UAs) gradually change their UX to display non-secure origins as affirmatively non-secure," the team writes in its blog post. The post continues, "the goal of this proposal is to more clearly display to users that HTTP provides no data security."

"We all need data communication on the web to be secure (private, authenticated, untampered). When there is no data security, the UA should explicitly display that, so users can make informed decisions about how to interact with an origin."

Users always compromise between their security and the flexibility/freedom while browsing the Internet. Now when I talk about Security, it means to reduce and lessen the online attack vectors, which generally minimizes our freedom to use some or more features.

The security team also remarks that HTTPS traffic usually produces a change to the user interface notification like new address bar indicators for the various browsers, yet insecure HTTP traffic does not. The security indicators and warnings are supposed to protect users from site-forgery attacks, such as man-in-the-middle attacks or ’phishing’ sites.

"We know that people do not generally perceive the absence of a warning sign," the Google Chome Security Team wrote. "Yet the only situation in which web browsers are guaranteed not to warn users is precisely when there is no chance of security: when the origin is transported via HTTP."

The researchers’ team suggests that browsers instead define three basic sates of transport layer security:

Secure (valid HTTPS, other origins like (*, localhost, *))
Dubious (valid HTTPS but with mixed passive resources, valid HTTPS with minor TLS errors)
Non-secure (broken HTTPS, HTTP)

More specifically, Google is encouraging user agent (UA) vendors to take a phased approach to implementing these changes given the needs of their users and their product design constraints.

"Generally, we suggest a phased approach to marking non-secure origins as non-secure," the team wrote. "For example, a UA vendor might decide that in the medium term, they will represent non-secure origins in the same way that they represent Dubious origins. Then, in the long term, the vendor might decide to represent non-secure origins in the same way that

they represent Bad origins."

This latest move by the search engine giant could push more sites to HTTPS by default, because the more encrypted your website traffic is, the better it will be trusted by user and prioritize in the Google’s search engine result. The post says that Google will "intend to devise and begin deploying a transition plan for Chrome in 2015."

Leaked Windows 10 Build Unveils Cortana, Xbox App

Windows 10 has given us another work-in-progress peek at itself, albeit through an unofficial and leaked build.

Popping up online on Sunday, the sneak peek dubbed 9901 gives us an early look at some of the things we’ll likely see in the flavor of Windows 10 that Microsoft is expected to reveal on January 21. So far, Microsoft has offered users a Windows 10 Technical Preview. But the leaked build and the official build due in January are reportedly more consumer-oriented.

Windows 10 is still very much in the early stages, but each new build of the Technical Preview has shown minor tweaks and new features. Part of the goal behind Windows 10 is to make people forget Windows 8, which upset users who were accustomed to the look, feel and features of Windows 7. As such, Windows 10 is restoring the Start menu, tweaking Windows Store apps so you can run them in resizable windows from the desktop and offering other surprises to win back disgruntled PC users. The builds released so far also show a tighter integration among the various features in Windows.

Cortana is one of the features taking the stage in the new build, according to The Verge. Microsoft’s voice assistant resides at the top of the Windows 10 search interface and offers access to your notebook, reminder and other features. In short, the Windows 10 edition of Cortana takes many of its cues from the Windows Phone version.

The new build also adds a new Xbox app, The Verge said, which brings you an entire Xbox experience. You’ll be able to see your friends list, achievements, activity feed and the Xbox store.

The Windows Store has opened its doors to more content as well. Beyond offering apps, the store in the new build sells music, movies and TV shows. That could mean Microsoft may do away with the separate Xbox Music and Xbox Video stores and add all that content to the Windows Store.

One of the frustrating aspects of Windows 8/8.1 has been the split between the familiar Control Panel and the new Settings screen. In some cases, you have to return to the Control Panel to tweak a certain setting. In other cases, you head toward the Settings screen. Several settings can be adjusted in either place. That confused users who didn’t know where to go to change a setting.

In the new build, the Settings screen looks more like the traditional Control Panel, according to The Verge. Also, the Settings icon no longer appears on the Charms Bar. Microsoft clearly is aware of the confusion among its users and seems headed toward integrating access to key settings in one place.

Microsoft is expected to release the completed consumer version of Windows 10 to the public sometime in late 2015.

Microsoft: We Have More Than 1.5 Million Windows 10 ’Insiders’

As of December 17, more than 1.5 million people have registered as "Windows Insiders" who can test Windows 10, according to Microsoft officials.

Microsoft Of those 1.5 million, 450,000, about 30 percent, are "highly active" testers putting the preview build of Windows 10 client through its paces daily, officials said in a new blog post.

Officials said Windows 10 testers are using Windows 10 test builds more actively than participants in preview and beta programs for Windows 7, 8 or 8.1. Microsoft has fixed almost 1,300 Windows 10 preview bugs reported and/or up-voted by testers, officials added.

Back in mid-October, shortly after Microsoft released the first public Windows 10 Technical Preview build, Microsoft said 1 million people had signed up as Insiders to test Windows 10.

When they released its second preview update to the Windows 10 Technical Preview in November, Microsoft execs said the next officially sanctioned Windows 10 preview update would be in early 2015. There have been a couple of unsanctioned leaked builds since then, the latest of which (Build 9901) shows off some of the UI changes Microsoft is expected to make part of its upcoming consumer-focused preview in January.

The reason for the lapse in what was shaping up to be monthly officially-sanctioned test builds, was explained by Gabe Aul, head of the data & Fundamentals Team in Microsoft’s Operating Systems Group (OSG):

"We’ve been very hard at work putting together a great build for you that includes a bunch of new features and improvements. As all of those payloads came in we needed to stabilize code, fix any integration issues, and ensure all of the new UX is polished. We’re really focused on making the next build something that we hope you’ll think is awesome. In fact, just so that we have a *daily* reminder to ourselves that we want this build to be great, we even named our build branch FBL_AWESOME. Yeah, it’s a bit corny, but trust me that every Dev that checks in their code and sees that branch name gets an immediate reminder of our goal." (FBL stands for Feature Build Lab.)

Microsoft is expected to release its next Windows 10 Technical Preview - with more consumer-focused features enabled - in late January, possibly on January 21 during its Windows 10 "Next Chapter" reveal event in Redmond.

Microsoft also is expected to show off at that event its Windows 10 mobile preview, which is expected to run on Intel- and ARM-based tablets, as well as Windows Phones. Microsoft’s OSG is hustling to make the mobile preview available to testers by January 21 or shortly thereafter, sources say.

Teens Continue To Flee Facebook

Facebook is no longer as cool a place for teenagers to hang out, according to a new report.

The percentage of teens ages 13 to 17 who use Facebook in the United States fell to 88 percent this year, says a report based on a survey conducted by research firm Frank N. Magid Associates. That number revealed a drop from 94 percent in 2013 and 95 percent in 2012.

But use of Facebook also showed a decline among all the other age groups examined in the study. In total, Facebook's popularity dipped to 90 percent this year from 93 percent the past two years.

Facebook has been facing a negative impression that it's no longer the in-thing among teenagers. Other surveys have found that teens have been cutting back on their Facebook use in favor of other socially-networked sites, such as Instagram, which, ironically, is now owned by Facebook.

In October 2013, the company's Chief Financial Officer David Ebersman said that daily Facebook use among younger teens declined from the second to the third quarter. Retaining the teenage market is important for Facebook not only to appear cool and vital but also to hang onto a younger audience to which it can sell products promoted on the site.

But others have dismissed any concerns that Facebook is losing appeal among teens. In November of 2013, Chief Operating Office Sheryl Sandberg said "the vast majority of US teens are on Facebook, and the majority of US teens use Facebook almost every day." A survey from research firm Forrester conducted this past June found that Facebook was still the favorite social network among more than 4,500 teens (aged 12 to 17) polled in the US.

Still, there are reasons Facebook may not be as popular as it once was among the teen crowd and people in general, according to Frank N. Magid's survey. Among all of those polled, 16 percent said Facebook was trendy, 18 percent said it was fun and 16 percent said it was informative. But only 9 percent said it was safe and 9 percent said it was trustworthy.

Facebook has often gotten into trouble over privacy issues. The site has been criticized in the past for adding or changing certain features or revising its privacy policy in ways that triggered concerns that user privacy was not being considered. The company has attempted to be more sensitive to such concerns, but clearly people are still wary, according to the Magid survey.

So if teens and adults aren't on Facebook as much, what are they doing online? The poll found an increase in popularity among instant messaging apps. Among those surveyed, 18 percent use Snapchat, 17 percent use Apple's iMessage, 9 percent use WhatsApp and another 9 percent use Google Hangouts.

What was the most popular messsging app? Facebook Messenger among 40 percent of those polled.

Conducted this past September, Magid's survey reached 1,934 people, but only smartphone users were polled. Facebook itself holds more than 1 billion users worldwide, so the survey numbers represent a tiny fraction of the total population.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.